copy to DD(CSA)
12/8

15(I)

TOP SECRET "U"

TICOM/I-58

9. 7/VI and 1

INTERROGATION OF DR. OTTO BUGGISCH OF OKW/CHI

Attached are (a) the translation of a paper written by Dr. Buggisch on his cryptanalytic life history, and (b) notes amplifying the above based on the interrogation of Buggisch carried out at Revin by Major Bundy, Captain Campbell and Captain Lawrance in July 1945.

Major Bundy reports on Buggisch as follows:-

"Our personal impression remains that he is an A-minus man, whose knowledge is in large part second-hand and by familiarity (i.e. being in the same room with others). He does know about a lot of work that was done--the general lines and result--but his own work seems to have been competent rather than outstanding.

"He is a hard man to handle in oral interrogation as he jumps from one subject to another and talks very fast. His written work is well-written and systematically arranged to cover all points."

Buggisch is now writing a full report of his work on the Russian "X2" voice scrambling device

TICOM
8 August 1945

No. of pages 9
Copy No. 12

Distribution

British

1. Director
2. D.D.3
3. D.D.4
4. D.D.(N.S.)
5. D.D.(MW)
6. D.D.(A.S.)
7-8 A.D.(C.C.R.)(2)
9. Lt.Col. Leathem

TICOM

10. Chairman
11-12 S.A.C.(2)
13. Cdr. Bacon
14. Cdr. MacKenzie
15. Cdr. Tandy
16. Lt.Cdr. Manson
17. Lt.Col. Johnson
18. Major Seaman
19. Lt. Eachus
20. Lt. Vance
21. Capt. Cowan
22. Lt. Fehl
23-24 Ticom Files (2)

U.S.

25-26 OP20-G (2) (via Lt. Pendergrass)
27. G-2 (via Lt.Col. Hilles)
28-29 S.S.A. (2) (via Maj. Seaman)
30. Director, S.I.D. USFET (via Lt.Col. Johnson)

Additional

31. Maj. G.W. Morgan
32. Mr. Sainsbury, Berkeley St.
33. Dr. Tunny TURING
34. Lt.Col. Pritchard
35. Mr. Twinn

Dr. Otto Buggisch. OKW/Chi

The most important dates in my activity

as cryptanalyst

May 40 to July 40. W/T Listening Interpretation Station of Army Group 'C' - BAD SCHWAIBACH, KREUZNACH, SAARBRUECKEN. Hptm. Mettig - Hptm. Franz - Insp. Kuehn. F90, F110, diagonal write-out transposition, C36.

20/7/40 Summer 40. Attached to W/T Listening Interpretation station BERLIN (rest of W/T Listening Interpretation Station, i.e. specialist parties for RUSSIA and BALKANS) Bendlerstr. 29/30. Major Wollman, Hptm, Meilbeck. Course, completion of 2 works on the C36. First acquaintance with OKW/Chi (Doktor Huettenhain, Oberinsp. Menzer). M40.

About September 1940. Transfer to Russian specialist party (Bleschke, Dettman, Torunsky, Liedtke). Practice messages, 4 figure code (Olowo), 5 figure code.

Oct. or Nov. 40. Return of the W/T Listening Interpretation Station from FRANCE (Obstlt. Kettler, Major Jung).

About January 1941. Transfer to BALKANS specialist party (Reg. Rat. Bailovic) Greek 5 figure code, transposition. 2 memoranda - JUGOSLAV code.

About 1/2/41. Transfer of all cryptanalysts from the W/T Listening Interpretation Station to 'Inspectorate of Signal Troops' (In 7, Head of Department Obstlt. Hassel). Founding of section (Spring 1941) VI from elements of former section IV and personnel now joining from the W/T Listening Interpretation Station, Head of section Major Mang. Move to Schellingstr - lack of work in BALKANS specialist party.

June 41. Military incorporation of all soldiers in In 7/VI working on cryptanalysis in the newly formed 'Signals Recce Coy.', later Signals Recce Abt. The RUSSIAN specialist party is again subordinated to the W/T Listening Interpretation Station and goes with it to LOETZEN.

Beginning of July 41. Attached to RUSSIAN specialist party at LOETZEN. Chiefly 5 figure material. OK40. Low-grade systems. K37.

Nov. 1941. Return to BERLIN to In 7/VI. Transfer to FRENCH specialist party (Matthekirchplatz 4). There until August 42. (Hatted diplomatic 5 figure code of De Gaulle, SWISS machine messages. Acquaintance with Enigma and Type-X documents; Ober Reg. Rat Kunze of the Foreign Office, FRENCH diagonal write-out transposition (Central AFRICA de Gaulle)).

Beginning of 1942. Major Mettig head of section. Disbanding of Signals Recce Abt. Incorporation of soldiers engaged on cryptanalytic work in 4 Coy. (Evaluation Coy.) of Signals Working Abt. (Chef. H. Ruest. u. B.d.E. ('Intellectuals' Coy').

Summer of 42. First detailed investigation (Dr. Doering) into cypher teleprinters T52 a, b, c, SZ 40. Completion of the works of Dr. v. Denffer and Hilburg on B 211.

About August 42. Surrender of a few mathematicians to section IV as "inventors" of new systems. Reorganisation of the specialist parties of section VI. My transfer to the newly formed machine specialist section. Extensive investigation into cypher machine 41. First acquaintance with Wa Pruef 7/IV (Dr. Pupp). Call-sign systems, weakness of the double Playfair.

October 42. Official visit to Wanderer Werke, CHEMNITZ about machine 41.

November 42. Beginning of investigations into machine 39 (Naval). Many discussions, official visits T & N, FRANKFURT/Main. Thoughts on mechanical aids to cryptanalysis.

In the course of the year 42 (?). Strip system solved in the USA specialist section.

Spring 43. General investigations into 'small technique [TECHNIK]' (Hagelin)*. 1 example of the BC 38 received from Wa Pruef 7/IV together with the statement that Hagelin was working in America (Dipl. Ing. Voss at STOCKHOLM). Occasionally some investigations into Enigma-machine 39 and consideration of the technical cypher part of a future German Standard Cypher teleprinter [SFM].

Roughly end of 42 or beginning of 43. Reappearance of C 36 messages in De Gaulle traffic. Decoding by means of the method developed earlier by Dr. Denffer; likewise B 211 messages appear, which however do not decode according to the theoretically worked out method.

Summer 43. Works of Dr. Luzius - Dr. Kochendoerffer on the crib problem with the convertor 209. First key recovery from a crib. Major Lechner Head of Section In 7/VI. Occasionally conferences with OKW/Chi on BC 38, Enigma, cypher teleprinter (Dr. Stein, Hassenjaeger). Breaking of CROATIAN enigma. Captured specimen of convertor 209 from Italy - roughly about August 43.

In the course of the year 43. Renaming of In 7/VI as 'Department of Signals, Signals Recce Section (AgN/NA)'.

October 43. Move of office to JUETERBOG.

Winter 43/44. Investigations of Dr. Doering - Troebliger into RUSSIAN cypher teleprints, cribs, results of the Forschungsamt. Enigma: crib problem, bigram system. Convertor 209: column separation [Spaltentrennung]. C 36 messages with complicated encyphering technique, solved in the spring (Le zouave du pont d'Alma a dit). Theoretical lectures: depth problem, X^2 and W^2 method.

November 43. Discussion with Korvetten Kapitaen Jaeckl.

Jan./February 44. Discussion at KOETHEN on cypher, teleprinter T 43.

First half of the year 44. Investigations into weaknesses of the Naval Emergency Key (Kapt. z.S. Beegemann)(Freg. Kapt. Singer). Weaknesses of the Army Enigma system. Compromise of key through message setting and question of possibility in principle of breaking by means of enormous employment of machinery.

LÜCKENFÜLLER** and STECKERUHR.

Wicher case.

22/6/44 - April 45. Attached to Communications Experimental Station [NVA], STAATS (Army Ordnance Branch, Pruef 7/IVe), (Obstlt. Weidemann, Dr. Lotze), for the purpose of mathematical treatment of ciphony systems. Almost exclusively Russian X^2 system. Undulator [FREQUENZ-SCHREIBER], lack of equipment. Theoretical investigations into the construction of Tigerstedt keys. Brief acquaintance with the work of specialist section c (A3 and A9).

Autumn 44. Attachment suspended; transferred from AgN/NA to OKW/Chi/IV; returned to STAATS. 'Chi-conferences' in BERLIN at the instigation of General Gimmler.

24/1/45. 3 lectures at OKW/Chi on ciphony. Followed by official visit to EBERMANNSTADT, Feuerstein laboratory, to become acquainted with the proposed German systems.

Beginning of March 45. American/English ciphony apparatus from a captured Mustang a/c restored to working order by German Aeronautical Research Institute (Dipl. Ing. Vegemund) and its working described. The investigations begun at Pruef 7/IVe could not be carried very far owing to the general disorganization then beginning.

-- -- -- * * * -- -- --

Notes by translator:

* It is perhaps relevant to note that the Swedish firm A.B. Cryptograph Stockholm produced an early type of Hagelin machine known as TEKNIK cryptograph machine. It may be this that is referred to.

** LÜCKENFÜLLER referred to by Dr. Fricke as a device for varying turnover of wheels by means of adjustable plugs on perimeter in TICOM/I-20, page 4, paragraphs b) and d).

Footnotes to BUGGISCH career

A. Systems studied.

1. Machines.

C-36 - The theoretical analysis of this in 1940 developed two theoretical methods.

1) Based on frequency of K. as word separator.
2) Statistical - various, depending on the most usable feature of the traffic, low, high letters, etc.

The studies made by B. et al. were used by Oberinsp. Kuehn to forestall the introduction of the device into the German Army, as advocated by Major JUNG.

B. says the statistical method was later used in practice and needed 300 letters. He makes general statements about considerable later success with C-36, from 1942 on. (Not pinned down on this.)

B-211 - B. studied this in 1942 in detail, using the traffic of two years before. A theoretical solution was developed and back traffic actually solved. However, the method did not work in practice when B211 traffic was again encountered actually, and B. did not mention any new methods devised or any idea of how the machine may have been changed.

K-37 - A Russian machine, same principle as B211, but more primitive. A model was captured in 1941, and a theoretical solution worked out by HILBURG and Dr. v. DEIFFER. They found it could be solved on a 10 letter crib. The work remained purely theoretical as no traffic in the machine was ever received.

M40 - A little machine designed by MENZER. DÖRING and B. did security studies on it in 1940, found it moderately secure but it was never actually used. I think B. said this was a forerunner of the C41, but the motion of the wheels was not so irregular.

C41 - B. says this was MENZER's idea, and the technical side was worked out by PUPP of WAPRUEF 7. As far as he knows only the Luftwaffe used it for 10 figure traffic (weather?). The Army hemmed and hawed and never did adopt it.

ENIGMA - B. worked on both the Swiss and Croat models, the former in liaison with Dr. KUNZE of the Auswärtiges Amt. At the close of one session he mentioned an idea for using Hollerith machinery to try all positions of the ENIGMA. (Not pinned on this.) In 1942 B. knew of studies by others on both Typex and ENIGMA. (Again not pinned). The Typex one showed it hopeless. B. knows of the Lückenfüllerwalze and Enigma Uhr ideas, but how much he had to do with them is not clear. "FALL WICHER" - Report Poles solved it in 1939.

M209 - B. knows of theoretical studies on this from 1942 on, chiefly by SDF LUCIUS. B. himself did some work on it.

BC38 - Swedish Hagelin. (Their spies in Sweden told them the U.S. was adopting a Hagelin idea.)

GERAET 39 - This was B's personal specialty, worked on by him at intervals from 1942 on.

T52, a,b,c - B. knows of the studies made on this in 1942 by DÜRING chiefly. D. found it (T52c) could be solved on 1000 letters of text.

SZ40,42,etc. - DÖRING also studied the SZ40 in 1942 and showed its insecurity. Doubtful how much B. knows--certainly not his main line.

Russian Baudot - B. mentioned Döring's work, but he has not been drawn out on this. He has said only that he had nothing to do with it in his own WAPRUEF 7 period (1944 on) and that the machinery (presumably Steeple Claydon) was built by Lorenz. The research was under Ref. C/Gruppe IV of WAPRUEF 7.

2. Codes and miscellaneous

a. Russian - In September-December 1940, B. worked on a 4-figure code with heading OLOWO. No success. Says he could not get enough depth.

Russian 5-figure code. B. heard of successful work on this in 1940. When he returned to Russian work in 1941 he worked on a 5-figure code (OK40) described as that used by the High Command to Army Groups and Armies, 300 plus groups, enciphered by a table (no mention of "BLOCKNOT"). This code had so much traffic that it piled up as many as 12 depths at first. A new code came in in October '41, and depths were less thereafter. B. and other mathematicians were withdrawn from this work in Nov. 1941, and he states that the problem was handed over largely to the Hollerith section.

"Lower systems" - B. knows of these, but says they were mostly handled forward.

NKWD, Partisans, etc. - not questioned.

Speech-scrambling systems - see special note.

b. French - In 1941-42, B. worked on a 5-figure de Gaulle code (in liaison with Kunze of the Ausw. Amt)--not successful. A compromise revealed it to be transposed. No later success with this knowledge.

Also F90, F110, simple field codes successfully solved.

c. Greek - In early 1941, B. solved a 5-letter code with a 7-cyclic recipherment (period of 35). Just getting to operational speed when the campaign ended.

d. Hungarian - When B. was in Balkan Referat, DÖRING solved a Raster-type cipher brilliantly. (early 1941)

e. Jugoslav - In 1941 B. knows of the solution of a code enciphered in a new system. Diplomatic traffic. Also claims general familiarity with work on Mihailović and Tito systems, but says OKW/Chi did most of this.

f. Rumanian - B. generally familiar with 1941 work on these.

B. German Crypt Methods and Organization

Analytic Machinery

B. says Hollerith was highly developed on the Russian 5-figure problem. He also mentions special analytic machinery, notably photocell comparison machinery used by OKW, which he says was better than the OKH use of Hollerith for same purpose. His familiarity in this field seems general only. Note the mention in his life story of first thoughts in this direction in November 42. ("EZ-Hilfsgeraete")

Heereswaffenamt and Wapruef 7

B. worked with Ref. A. of Gruppe IV of Wapruef 7 from June 1944 on. This was under Dr. Lotze, who with Dr. Schone had worked on "voice de-scrambling" for a long time. B's work in this is being covered in Special Report 1 in preparation (on the Russian "X2").

B. also mentions Ref. C of the Gruppe, under Bau Rat KIERKHOFF, as the research agency for work on Russian Baudot. The subject was not pursued, as B. said he knew little about its work. A3 and A9 refer to 3 and 9 Channel Russian transmissions, and the devices to intercept them.

B. did not work with Liebknecht, as L. was engaged in the opposite end of the work, i.e. developing German voice scramblers. This was under Gruppe III (L. having moved over from Gruppe II). B. and L. agree in the statement that the technical end of regular cipher devices was handled at first by Gruppe IV, but in about 1942 was turned over to Gruppe III.

In addition to the X2 work and some work on Tigerstedt at the end, B. mentions a special intercept location of the Referat at STAATS in a cave, at which some 5-letter radio traffic (with "HELLO TEK" in preamble) from London to U.S. was intercepted. Not pursued on this. Knowledge seems general.

B. says his first period in the Wapruef 7 was painful and useless, as he found no mathematical application and did not know enough electricity. He got to know his way around better, but his descriptions of devices are still not exact.

(Ebermannstadt) B's only connection with Ebermannstadt was a three-day trip in January 1945, for the purpose of seeing "ERSCHWERUNGSGERAETE" and "WOBBELUNG", to get ideas for the work of Gruppe IV on intercept devices. He can give only the most general description of these. ("WOBBELUNG" may not be at E., but it was in and out of the conversation at this point.) B. was taken through E. by a Dr. GOING (deputy head?). He says he has no detailed knowledge of the projects, there, as none of them were connected with Gruppe IV. He kept referring us to Liebknecht. Though the lack of liaison between opposite ends of the same work may seem strange, we felt sure he was not hiding anything. (He certainly isn't bashful in other matters!) Hence our firm opinion that he would be no use at E., at least from the technical standpoint.

(Frequenzschreiber) B. talked much of one device being developed at Gruppe IV. (We are not clear whether it was part of his work on Russian "X2"--the report in preparation will clarify the point.) This was the FREQUENZSCHREIBER--described as a device for analyzing speech transmissions. These were taken down on a sound track and a picture of the harmonics produced. B. says it was designed for speech frequencies (3000-5000). His description, as in other cases, is that of a layman. He says the device could be used for separating the propellor noises of planes and thus distinguishing them.

Further on Russian Baudot - B. says that one Dipl. Ing. GRAEBERG came to Gruppe IV with him from IN 7/VI and was used to translate the intercepted clear text in Russian Baudot. "90% of it was unimportant."

Work on German Security

This is a pet subject with B. His story is that up to 1942 the machines and systems introduced were not checked mathematically for security. When DÖRING in that year pointed out the weakness of the early T52's to the higher-ups (FELLGIEBEL) it was decided to check all new devices. But the liaison on this was still bad ("tragisch-comisch") and even if IN 7/VI detected an insecurity it was very hard to get action. (B. says he knew of grave misuse of double playfair, Enigma, and in the Panzer formation codes.)

Conversely it was very hard to get action on new devices. Geraete 39 and 41 were both in development for years and had still not come out at the end. B. has the almost inevitable comments about the military non-technicians who blocked things. B. says: c/s systems were the special province of Dr. v. DENFFER (see supra) and that FRICKE also knew this subject well.

OKH Work on Agent Ciphers

B. says he knows little about this, as it was under a special Referat under Oblt VAUCK and was kept separate from the rest, with no technical liaison.

C. Personalities in German Signal Intelligence

As his life story shows B. has a good memory for names and is familiar with a wide variety of sections and the specialists in them.

Most of the names are already known. The one name for which he adds conspicuous lustre is that of Wachtmeister DÖRING. (Incidentally both HENTZE and KARRENBERG concur in B's estimate). Döring did many original studies and solutions, and B. rates him .. frankly above himself. B. also speaks highly of Sdf LUZIUS' work on M209 (again HENTZE concurs), and of PIETSCH. (Döring was with IN 7/VI in the Machine Referat with B. and at the end was in Ref 1A of Gruppe IV, of Gen der NA).

Another name of possible interest is Dr. v. DENFFER, both from B. and named by HENTZE as chief of ENTZIFFERUNG with Kdr 6 at the end.